

Statement of Thomas A. Sadaka, Special Counsel  
For Computer Crime and Identity Theft Prosecutions, Florida Office of Statewide Prosecution

Testimony Before the Subcommittee on Social Security  
Of the House Committee on Ways and Means

Hearing on the Preventing of  
Identity Theft by Terrorist and Criminals

November 8, 2001

Mr. Chairman and members of the Subcommittee, my name is Thomas Sadaka and I am Special Counsel to the Statewide Prosecutor of Florida for Computer Crime and Identity Theft Prosecutions.

The Florida Office of Statewide Prosecution is charged with the investigation and prosecution of multi-circuit organized crime and to assist other law enforcement officials in their efforts against organized crimes. Identity theft is among the cases handled by the Office and is currently the focus of a great deal of the resources of the office.

The Office of Statewide Prosecution was instrumental in aiding the Florida Legislature in the drafting and passing of a statute criminalizing the unauthorized use of another's personal identifying information. As a result of our involvement in this arena the Statewide Prosecutor, Melanie Ann Hines, was invited by Governor Jeb Bush to sit on the Governor's Privacy and Technology Task Force where the needs of technological advancements were balanced against issues of social security number abuse, public records abuse and general identity theft. As a result of the report generated by the Privacy and Technology Task Force, Governor Bush requested the empanelment of a Statewide Grand Jury to specifically focus on identity theft issues and what the State of Florida can do to combat this epidemic. The Office of Statewide Prosecution also serves as the legal advisors to the statewide grand jury. Since July, the Statewide Grand Jury has been devoting one week each month to the investigation of identity theft related cases.

Additionally, the Office of Statewide Prosecution has partnered with the Florida Department of Law Enforcement (FDLE) in an identity theft task force where special agents of FDLE have been assigned exclusively to the investigation of large scale identity theft cases. Cases generated by this partnership have been presented to the statewide grand jury and since July have resulted in the arrests of numerous individuals and the dismantling of several criminal organizations with identity theft losses in excess of one million dollars.

This Subcommittee is well aware of the vast impact identity theft has on our society. States are scrambling to fashion laws to criminalize this conduct and law enforcement is quick on the legislative heels to learn how to effectively investigate and prosecute these crimes. Identity theft case investigations are time and resource demanding and are impacting heavily on already budget tightening law enforcement agencies.

The victims of identity theft face their own unique problems in rectifying the damage to their good names, their credit; and restore their lives while dealing with a criminal justice system that is heavily imbued in the learning curve.

Federal, state and local law enforcement are developing a proficiency in the investigation of identity theft cases and the private sector is becoming a bit more accustomed to dealing with and assisting law enforcement and the victims of identity theft. So while the “after the fact” dealings are getting less cumbersome, the issues of prevention are becoming more important.

Society is becoming well schooled in the idea that individual social security numbers are extremely important and valuable. As such, we don’t generally carry our social security cards on our persons any longer, and we take some precautions with our personal identifying information. What society has not become well schooled in is how readily available this information is to the would be identity thief through numerous sources.

It is well known to this Subcommittee how the social security number has become the de facto national identifier and is relied upon heavily by the financial industry, medical community, insurance industry, educational institutions and state and local government as a means to uniquely identify the customer. Each one of these entities reproduces the social security number within their own files and generated documents and makes this information available to others in some form. In spite of the fact that we don’t carry our social security cards, the vast majority of us have our social security numbers emblazoned upon our medical insurance cards in the representation of our policy number. There are still a vast number of driver licenses from the various states in circulation that have the holder’s social security number referenced as their license number.

Through the use of the Internet and the attendant speed at which information travels, the ability to gain access to personal identifying information, social security numbers and the ability to exploit that information from the perceived anonymity of a keyboard has empowered a new generation of identity thieves who have in turn made identity theft the fastest growing crime in the world. To further fuel this ability, we have information of lists of names and social security numbers routinely being auctioned off to the highest bidder on the Internet.

The push to put court files and other public records online only operates to increase the pool of information available to the identity thief. Court records are particularly attractive to the identity thief as they are, by nature, filled with personal identifying information, including social security numbers, ready for the exploit. Requiring the supplier of these records to redact social security numbers and other personal identifying information would be an immense undertaking and require far more resources than those agencies currently possess.

Through the investigation and prosecution of identity theft cases, the use of the social security number is constant. The identity thief relies more on the social security number of others than on any other personal identifying information. Evidence has shown misspelling in names, inaccurate dates of birth and incorrect addresses, however, the identity thief has success as long as they utilize a valid social security number.

When a living individual becomes the victim of identity theft, there is some ability on the part of the victim to intervene to stop the fraud. On average, victims become aware of the theft within a year of the occurrence with a great deal of victims becoming aware within a month. These victims have the ability to notify the consumer reporting agencies and the financial industry that their personal

identifying information has been compromised. Through fraud alerts and other overt acts on the part of the victim, the ability to continue the fraud is hampered. This is not the case when a deceased individual's social security number is utilized. In some instances, this type of fraud may never be discovered.

As you are aware, the Social Security Master Death File is made available to the public and private sector to determine if a social security number supplied by an applicant for credit, government benefits, state issued driver license or identification card, and the like, has been reported as belonging to a person who is deceased. In a study of state issued driver licenses and identification cards, we have learned that among those states that conduct some form of information validation, generally use the Master Death File to determine the validity of the supplied social security number.

If a terrorist or an identity thief provides a social security number of a deceased individual to a state driver license administrator, prior to the updating of the Master Death File, then it is highly likely that that individual will be successful in their endeavor to obtain a state issued ID. Once that ID is issued, the possessor will be able to use it for identification until it is lost, confiscated or expires. Needless to say, this false identification will be in use for years and the downstream effect or consequence could be immeasurable.

All efforts need to be made to increase the speed at which the Social Security Master Death File is updated. Identity thieves rely heavily on obituaries and the up to six month lag time between death and the inclusion of the social security number in the Master Death File for the commission of their crimes. The current distribution method of mailing the list out on tape would seem to be outdated and obsolete.

#### Recommendations:

Since we all recognize the wide spread use of the social security number for purposes that far exceed the original intent, steps must be taken to provide those relying on the social security number with access to validation and confirmation information or to prohibit its use to anything beyond the original purpose and intent.

Current efforts to make online verification of social security numbers available to state governments, particularly driver license administrators, has not been effective. Very few states currently avail themselves of any real time verification of social security numbers provided by applicants. Several states interact with the Master Death File, but that interaction is not real time and as previously illustrated, once the DL or ID card is issued, it is nearly impossible to remove from the stream of commerce. Infrastructure enhancements must be employed to facilitate the interaction of states with the social security database to immediately confirm the validity of the supplied social security number and if it belongs to the person presenting the information.

Identity theft is an epidemic. The onus is upon the government to do everything in its power to prevent government's own information, primarily the social security number linked to other personal identifying information, from further victimizing her citizens.

Laws limiting the use of the social security number and punishing its unauthorized use or dissemination need to be enacted to provide the ability to prosecute those who would sell names and

social security numbers to the highest bidder.

On a final note, I would recommend a campaign to educate the public as to the proper use of a social security number and to question those that request it for daily business transactions, school volunteer forms, health club memberships, and the like.

Thank you for the opportunity to be here today. I would be happy to answer any questions.